



THREAT INTELLIGENCE
REPORT

BitXLucky Scam Casino Panel

59-domain fake casino network stealing from both victims and its own affiliate workers

PUBLISHED

March 08, 2026

THREAT TYPE

Scam Casino Panel

CLASSIFICATION

TLP:CLEAR

SEVERITY:
HIGH

PHISHDESTROY RESEARCH DIVISION • [HTTPS://PHISHDESTROY.IO](https://phishdestroy.io) • REPORT ID: PD-BITXLUCKY-2026-03-08

59

DOMAINS

3

IPS

1000+

WORKERS SCAMMED

Next.js/NestJS

TECH STACK

Executive Summary

The BitXLucky Scam Casino Panel is identified as a low-quality fake casino and sportsbook platform. It is operated by a group of threat actors using multiple Telegram handles. The panel is currently active and utilizes domains such as [bitxlucky.com](#) and [bitxlucky.vip](#). The platform has been reported to have at least two domains and an unknown number of victims due to its deceptive practices.

The platform is designed to steal registrations from workers, routing all stolen funds to the operator. The current status of the platform is active, with ongoing fraudulent activities targeting both users and affiliates. The infrastructure includes multiple IP addresses and a tech stack involving Next.js and NestJS.

Threat Actor Profile

TELEGRAM HANDLE	ID	REGISTRATION DATE	ROLE
@memorycrypto	6938945548	December 2023 / March 2024	Support
@abszv, @netyvremeny, @imsot1r3d	6684395748	2023-12-16 to 2026-01-31	Support / Project Member

Known infrastructure connections include the use of Cloudflare for CDN and IP addresses such as [77.110.103.90](#) and [176.46.152.13:3000](#).

Technical Infrastructure

COMPONENT	DETAILS
Frontend	Next.js (React) with Turbopack bundler
Backend	NestJS (Node.js)
Auth	JWT HS256
CDN	Cloudflare
Hosting	IP addresses 77.110.103.90 , 176.46.152.13:3000 , 77.221.151.196

API endpoints include:

- [POST /api/promocodes-api/custom](#)
- [POST /api/promocodes-api/generate](#)

- GET /api/promocodes-api/{name}
- PATCH /api/promocodes-api/{name}
- DELETE /api/promocodes-api/{name}
- GET /api/promocodes-api/{name}/stats

Panel sections include Home, Users, Deposits, Live saport, Promo codes, Logi, Domains, Payments, API, Sapport, and Settings.

Attack Chain / Scam Flow

1. Victims are lured to the platform through fake promotional campaigns.
2. Users register on the platform using a promo code, but registrations do not appear in the worker panel.
3. Victims are prompted to make a minimum deposit of 100 USDT.
4. Upon attempting withdrawal, victims receive an error message stating their withdrawal is flagged as high-risk.
5. Victims are instructed to make a confirmation deposit to proceed with the withdrawal.

Indicators of Compromise

DOMAIN	STATUS
bitxlucky.com	Active
bitxlucky.vip	Active

IP	ORGANIZATION/COUNTRY
77.110.103.90	Unknown
176.46.152.13:3000	Unknown
77.221.151.196	Unknown

WALLET ADDRESS	CHAIN
Not available	Not available

TELEGRAM ACTOR	ID
@memorycrypto	6938945548
@abszv, @netyvremeny, @imsot1r3d	6684395748

Victim Impact

Geographic breakdown data is not available. Financial impact is significant due to the theft of registrations and deposits. Promo code analysis reveals the creation of 8 promo codes, including VEJ4H7 and HBQRNQ .

MITRE ATT&CK Mapping

TACTIC	TECHNIQUE ID	TECHNIQUE NAME	EVIDENCE
Initial Access	T1078	Valid Accounts	Use of promo codes for registration
Credential Access	T1556	Modify Authentication Process	JWT HS256 for authentication
Exfiltration	T1041	Exfiltration Over C2 Channel	Stealing registrations from workers

Countermeasures

- End users should avoid engaging with suspicious online casinos.
- SOC teams must monitor for traffic to known malicious domains.
- Registrars should investigate and suspend domains involved in scams.
- Law enforcement agencies need to track and dismantle the infrastructure.
- Use the [PhishDestroy free domain scanner](#) for domain risk assessment.
- Refer to the [DestroyList open-source blocklist](#) for updated threat indicators.

References

- [PhishDestroy threat intelligence platform](#)
- [Free domain risk scanner](#)
- [DestroyList community-maintained blocklist](#)
- [ScamIntelLogs evidence archive](#)

[Download IOCs \(CSV\)](#)

PhishDestroy Research Division

770,000+ threats tracked • 500,000+ domains blocked • 0.01% false-positive rate

[phishdestroy.io](#) • [Free Scanner](#) • [DestroyList](#) • [ScamIntelLogs](#)

© 2019-2026 PhishDestroy. CC BY 4.0 • PD-BITXLUCKY-2026-03-08